JWR-99-002
March 1999

The Navy and the Infosphere

Michael Vlahos and Dale Pace

This document may be accessed electronically at
<**http://jhuapl.edu/cybertech**>.

JOHNS HOPKINS
UNIVERSITY

Applied Physics Laboratory

11100 Johns Hopkins Road
Laurel MD 20723-6099

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 01031999	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle The Navy and the Infosphere	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Johns Hopkins University Applied Physics Laboratory 11100 Johns Hopkins Road Laurel MD 20723-6099	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 34	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	3/1/99	Report

4. TITLE AND SUBTITLE
The Navy and the Infosphere

5. FUNDING NUMBERS

6. AUTHOR(S)
Michael Vlahos, Dale Pace

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This report explores implications of the Big Change in society, business, and military operations that is expected to emerge from the Infosphere. After treating broad societal possibilities, the study narrows its focus to their possible impact on the Navy and on Defense-related research organizations like The Johns Hopkins University Applied Physics Laboratory (JHU/ APL).

This report is an occasional paper of the Joint Warfare Analysis Department (JWAD) of JHU/APL. The ideas in this report are intended to stimulate, perhaps provoke, serious thinking about the future. Not everyone will agree with its ideas. Therefore, it should be noted that this report reflects the views of its authors and does not necessarily imply concurrence with those views by JHU/APL or by any other organization or agency, whether public or private.

14. SUBJECT TERMS
INFOSEC

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

ABSTRACT

The Infosphere is a shorthand for the fusion of all the world's communications networks, databases, and sources of information into a vast, intertwined, and heterogeneous tapestry of electronic interchange. This report explores implications of the Big Change in society, business, and military operations that is expected to emerge from the Infosphere. After treating broad societal possibilities, the study narrows its focus to their possible impact on the Navy and on Defense-related research organizations like The Johns Hopkins University Applied Physics Laboratory (JHU/APL).

This report is an occasional paper of the Joint Warfare Analysis Department (JWAD) of JHU/APL. The ideas in this report are intended to stimulate, perhaps provoke, serious thinking about the future. Not everyone will agree with its ideas. Therefore, it should be noted that this report reflects the views of its authors and does not necessarily imply concurrence with those views by JHU/APL or by any other organization or agency, whether public or private.

The Authors

Michael Vlahos is a consultant to JHU/APL who has written extensively about the Infosphere and is associated with the United States Internet Council. Previously he directed the Security Studies program at The Johns Hopkins University School of Advanced International Studies, was Director of the State Department's Center for the Study of Foreign Affairs, and has worked with the Center for Naval Analyses and with the Progress and Freedom Foundation. His e-mail address is **mevlahos@aol.com** .

Dale Pace, a specialist in operations research and Defense analysis, is a member of the JHU/APL Principal Professional Staff who coordinated the first series of the JHU/APL Cyber Tech Seminars. Previously he taught in the graduate technical management program of The Johns Hopkins University Whiting School of Engineering and was the JHU/APL liaison with the Naval War College, where he developed and taught an elective course on technology and naval warfare. His e-mail address is **dale.pace@jhuapl.edu** .

CONTENTS

To return to the Table of Contents click on the page number

INTRODUCTION

The emergence of effective communications networks has changed how people connect, how business is done, and how military forces operate. Everyone seems to understand this: global networks are changing every aspect of life. But do we understand how these networks themselves are changing? The Johns Hopkins University Applied Physics Laboratory (JHU/APL) has been exploring the transformation of a global network ecology from what was seen as a communications medium to a truly social environment, with emphasis upon the potential impact of this transformation on research organizations and military operations. This social environment is a new human place where people meet, interact, and do business. The pace of development—or the rate of "track-laying," to use a benchmark image from the Industrial Revolution—suggests the emergence of a mature Infosphere Ecosystem within 20 years. For military forces, this not only enhances traditional military operations but becomes, potentially, a new arena of operations, even of battle.[1] The significant element of this hypothesis is the potential for this new place in cyberspace to grow into the focal center of human activity and global business and, by extension, into the decisive theater of future military operations. We call this place the Infosphere.

This report explores how the Infosphere might evolve, how its development might affect military operations, how the Navy in particular might be affected, and, finally, how Defense-related research and development institutions like JHU/APL could be affected. Appendix B looks at some of JHU/APL's Infosphere activities.

This report makes no apologies for its breadth and sweep. It is impossible to talk about the big change the Infosphere brings to the Navy without talking about the big change the Infosphere brings to the whole Defense world. But big change, even in military societies and war, is just a small part of the change rippling through all society: the truly big change that the Infosphere potentially brings to our very reality. So the story of the Navy and the Infosphere is really three interlocking stories. These stories should be told together, beginning with the biggest first, because the story of how society changes has such potential impact on *all* aspects of the Defense community. Only then does it make sense to tell the story of how the Defense world might change, and then, finally, how the Navy might change.

It might seem simpler, perhaps, to jump right to the Navy story, but the Navy story makes no sense out of context; it looks like a fable or tall tale, and its real significance might inadvertently go unnoticed. Not catching it all risks missing what is really important. So bear with us.

WHAT IS THE INFOSPHERE?

The Infosphere is a shorthand for the fusion of all the world's communications networks, databases, and sources of information into a vast, intertwined, and heterogeneous tapestry of electronic interchange.[2] The global fusion of networks changes the character of each individual network. Networks will no longer serve simply as the medium through which people in different places can communicate, enhancing their *in situ* activities. The global fusion of networks creates a network ecology—literally, a place in which people can gather and do business. People will be able to conduct their activities increasingly in the global network ecology[3]—the Infosphere.

The Infosphere is a shorthand for the fusion of all the world's communications networks, databases, and sources of information into a vast, intertwined, and heterogeneous tapestry of electronic interchange.

The Infosphere has the potential to gather people and knowledge together in one place. This is what makes the Infosphere so compelling. The place itself is not "real," meaning that it is not part of our normal, physical world. Operating in the Infosphere is disconcerting today, but people accept its alien environment because it offers tremendous advantages. It gives people the ability to meet anywhere, anytime. It gives people access to information from everywhere, all the time. And people can meet in groups, talk, trade, and decide things, just like they do *in situ*. The difference is that they are not site-bound.

Business transactions and financial exchange are already migrating to the Infosphere. It is poised to become the new global marketplace. People well-equipped to enter the Infosphere today are finding that they can do business there while dramatically reducing onsite overhead, happily pruning business travel, and exponentially expanding customer geography. Economic advantage is driving the evolution of the Infosphere.[4] Capital expansion and competitive awareness means that, in the near future, most enterprises in the developed world will be doing business in the Infosphere. As the Infosphere becomes essential to enterprise, it will become essential to most people as well. But people will not make the Infosphere a part of their lives simply because it is business. It must also be ratified in the life of society.

Creating societies through business enterprise is the decisive factor in the Infosphere's current development. Enterprises are taking their WANs and LANs and moving them into the ecology of the Internet. Call this the transcendence of the network, pulling the "office" into the Infosphere. New "intranet" cultures are evolving. Compartmentalized corporate societies are dynamically reconnecting with themselves and, in turn, with the wide world through the relational technology metaphors constantly being created for the World Wide Web. This means that from coffee mess to corporate plaza the new meeting ground of each corporate community will migrate from office places to intranet/extranet places. People will find they do business more effectively in the intranet and that they feel closer to their firms, their office-mates now in the ether. The first real communities begin here.

A replacement for the industrial-era ethos will be ratified through social relationships in Infosphere enterprise. This leading edge effect in cultural adaptation is not new. It was, in fact, integral to how American society adapted to the industrial big change. What happened then, and what should happen now, is that micro-behaviors, values, and norms established and ratified in business enterprise will be melded into a template for the value system of an Infosphere-centered society. Business is the conveyor, not the creator—our core cultural values are embedded in our societies of enterprise—and it is a powerfully effective conveyor of values in the American ethos. In the American experience, the establishment of norms by business is the path most accepted by Americans. The way to legitimacy for new social patterns in American life will be found in Infosphere enterprise.[5]

The human migration to the Infosphere represents an historical shift in several senses of significance. It is a true movement of human society to a new place, much like the colonizing of the New World, while still connected to the old. It is thus a migration from, but in addition to, the *in situ* and material patterns of all human relationships to something very different and more complex. This means a migration from long familiar patterns of culture. Human culture has always adapted to fit new environments. The change is often as difficult as it is exhilarating, because it involves discarding many cherished and familiar ways of life. But it is also ultimately comforting, because the high stakes we see in making the change work motivate us to find ways to preserve what is really important to us.

Peoples' migration to an alien environment requires a shift in social patterns and spirit. The

Infosphere seems to be about technology; people are still taught that the Infosphere is a communications network. Then they discover, on entering, that it is really a place—a place for them. Like any human place, architecture does not make a place, people do. The migration of people to the Infosphere depends in part on people seeing it as important to their life and work. But their willing migration also depends on people seeing it as a human place that is comfortable, familiar, and social. When people collectively reach this crest of recognition, their migration will quickly bring all of us to a cultural watershed. That is when the Infosphere will become suddenly central to the life of society.

The Infosphere changes us through a strange blending of technology and culture—strange, but not alien. We think of technology as something apart from us, as creating discrete artifacts that we put to use. But the Infosphere is not discrete; it is potentially all-encompassing. Technology's network ecology brings fundamental change to us. But we do the changing; we will decide what we want to be in the Infosphere. And the Infosphere is perhaps the most plastic, the most moldable yet of all human places. Advances in processing, networking, and delivering will allow us to extend and enrich the world of the Infosphere easily, without mortar and brick and building permits. And it is important to note that the Infosphere exists today, however primitive it feels to some. It exists because the mesh of network technologies, processing, operating, and data systems has expanded and matured to the point of beginning to create a place we can enter.

"Place" is essential to understanding the change. Big changes in human life—the emergence of cities and the Industrial Revolution—are expressed through a new web of social relationships and social meaning that themselves are expressed and understood within the metaphor of a new human place. The new tools build the new place, but what really changes is human society.[6] So the hypothesis that our new tools, information technology, are building a new place—the Infosphere—is consistent with the patterns and process of periodic historical shifts in human life.

INFOSPHERE AS BIG CHANGE

Pursuing this human migration, and the things that make it move, inevitably brings us to thinking about earlier great migrations. The emergence of the Infosphere suggests an historical shift, a fundamental change in human life on the scale of the Industrial Revolution. This change is so encompassing that it sweeps up all subcultures in society, including military societies, as well as affects how those subcultures do business. This overwhelming process needs to be explicitly described, because military societies today tend to see their path to the future as somewhat separate, even compartmentalized, from changes in the larger society and spirit of the age. The exact opposite rules in times of big change. Military societies and war itself get swept up in the totality of the big change.

The Industrial Revolution of the 19th century is a good reference point for showing how big change moves through society and, eventually, military society. We remember that transformation in life as the arrival of new artifacts, what we today like to call "technology." But these artifacts were simply a tool set that came to us all at once. The revolution was in how people put these new tools to work. Rails and steam were used to transform society. And transformation came, not from a single-minded plan but from the creation of a new social environment. Technology's tools created a new human place, and when people migrated to this new place, they changed not only how they lived but also how they saw themselves and how they related to others.

The creation of a new human social environment was the essential, central feature of the Industrial Revolution. The driving technology element of that transformation was

the railroad. The railroad was more than a simple transportation or communications system; it quickly became a living network of people. Railroads made possible a new human organization built around industrial cities—the hubs—served and sustained by the rail network.

One dominant social element, set first by early 19th century British society, was a cultural eagerness to take advantage of the economic opportunities of this network. Equally critical to the interaction of technology and society in creating a new human place was the willingness of ordinary people to migrate to the new industrial cities and endure the hardships there, because of the expectations that it would lead to a better life. Technological possibility and human aspiration worked in concert.

The fact of big change, combined with people's receptivity to it, ultimately created a pattern for change in civilian society. This pattern of social adaptation, which included changes in society's major public and private institutions, also came to include two of its most celebrated public organizations: the army and the navy. Whether we look at what happened in Britain or France or Germany or the U.S. or Japan, the pattern is unmistakable; military relationships and organizational patterns in the industrial era came to mirror similar new patterns in business and in public institutions.[7]

- Command structures and military management were modeled on the new business corporations. The Army and Navy reforms of the Progressive Era consciously borrowed from the management style and business practice of America's dominant industrial corporations.
- Military social organization quickly moved away from its traditional, familial pattern of identity and relationship—the way of life immortalized by John Ford movies as the U.S. Cavalry post on the Western frontier—to an operational structure that more closely resembled that of the modern factory.
- The national mobilization frenzy that swept the European powers at the beginning of this century soon entranced American military thought.[8] But this idea of mobilizing had little in common with the Levee en Masse of the Napoleonic Era or the American native tradition of the Militia as nation-in-arms. Rather, it spoke to the industrial vision of society organized around mass constituencies that could be orchestrated by command authority from above.

Today's big change may look very different from the transformations of the industrial era, but two aspects of it may come to look very familiar:

- People are migrating to new places because of the interaction of technology and society.
- Military societies are already sharing and reflecting the ways that a larger society is adapting to the change.

THE PATH OF EVOLUTION

The next change to consider is the actual way we get from here to there: the path of evolution. Military societies should recognize that where they will end up will to a large extent be determined by where American (even world) society ends up. Part of our problem today in confronting this path is a vision of the future leashed to today's agent of change. But today's change agent is merely the dominant force during this particular phase of a larger historical process of change. The path of evolution is really a series of steps, marked by distinct time periods, when a characteristic change agent dominates the scene. Today's change agent is of course the Internet, and so we see change made by the Internet, and where the Internet is taking us, as the change itself. But it is only the change agent for this phase of the Infosphere evolution.

Instead of the Internet as the instrument of our transformation (the counterpart of the railroad back then), the Internet, which to most

means the World Wide Web, is only the first Infosphere iteration, an embryo. Its main historical role will be seen as having created the network foundation for the Infosphere. This is an important distinction to make because the Internet is merely an enhancement to our lives, a supplement. It cannot serve as the agency of social transformation because its technology base is too limited, but it leads the way to the transformation.

There is a useful historical precedent that illustrates what the Internet means to big change. Before the railroad ever appeared, Britain already possessed a unique stagecoach/turnpike network that tied the country together. Hundreds of stagecoaches left London daily, and all parts of Britain could be reached in timelines reckoned in hours.[9]

This made late-18th century patterns of life better—better than any other place in the world—but did not fundamentally change those patterns. The stages moved people and post but not big cargoes. It created a national network but it was limited. But it did do three things:

- It successfully tested and validated a new network concept—rapid, reliable, scheduled national travel.
- Its success helped create a new market for this network; people now wanted to travel (it had been arduous and dangerous before) and could base much of their business on written correspondence.
- This desire created a real surge in demand which, in turn, pushed technology developments that make the next network—the railroad—possible.

And the railroad then proceeded to change everything. *The Internet today is doing the same three things*. Like the late 18th century British stagecoach network, the Internet started primarily as a people-to-people connection. It began as a single, government-sponsored "backbone" for communication between the professional elite—the ARPANET. It evolved into an extended set of online "lifestyle communities" among members who were already participating professionally in the Internet.[10] E-mail became an explosive phenomenon, and billions of messages are now sent over the net.[11]

But also like the stagecoach net, the Internet is showing the way to business—the equivalent of the "big cargoes" that the railroad net would soon haul as routine. An important insight should be that the Internet will evolve into the Infosphere as it becomes a primary place of business.

We are witnessing the rapid emergence of serious business activity on the Internet. It is this activity, the creation of enterprise environments, that will drive the evolution of the Infosphere and make it the next human place.

Stages of Infosphere Evolution. Phase 1: Business Drives Growth

Business enterprise is the force currently driving the evolution of the Infosphere. Before it was the Infosphere, it was the Internet, and its original driving force was military-strategic. The earliest progenitor of the Infosphere was the ARPANET, created by the Defense Department's Advanced Research Projects Agency. The Internet quickly grew beyond its original academic-military membership but remained an elitist network exclusively until the creation of the World Wide Web. The Web phase of the Infosphere's evolution was short but decisive. The Web itself had little quantifiable economic value, but it was wildly addicting. Demand for Web use drove Internet expansion from single backbone to a global network ecology. This laid the foundation for the Infosphere.

The Infosphere, as we are using that concept, began when a significant amount of business enterprise began migrating there to do business. The year was 1997. The process, gathering momentum month by month, can be summarized with almost elegant simplicity:

Network → Intranet → Extranet

The process began with the development of client-server networks designed to wire individual office environments, usually *in situ*. Over time, wider area networks emerged, but these were still closed networks, tying together an enterprise in pristine isolation.

Along came the World Wide Web, which immediately offered a new venue for enterprise to advertise to the world. Companies rushed to present themselves on the Web, establishing thousands upon thousands of corporate web sites. Then they discovered that the Web was a good way to network themselves; utilizing the Web allowed a distributed office environment with unlimited interconnections within an enterprise or institution. So corporate networks began to migrate to the Internet.

Then, suddenly, people saw how companies on the net could reach out and do business outside their intranet environment, by opening the intranet up and making it an extranet. The development of extranets means that these emerging corporate "worlds" can now connect with each other and with individual clients and customers.

This model of Infosphere evolution has three aspects that make it different from the railroad-building era. The Infosphere's enterprise-driven development means a very open, less regulated, and highly complex Infosphere mesh, which makes it potentially more robust and sustainable:

- It is in essence being built from the bottom up. The Infosphere is building itself up from business, from what works and is sustained by the market.
- Its growth is organic. Overall development is unplanned and takes on a kind of microeconomic aspect, dependent on a multitude of individual decisions, each reflecting what an enterprise can do effectively in the Infosphere. So the Infosphere's growth will naturally tend to equal its actual business effectiveness.
- What is forming can be seen as a network ecology. As enterprises network with each other, the demand for business-to-business and people-to-business transaction capacity will grow. But this is fundamentally different from the earlier railroad network because the Infosphere's architecture fosters inhabitation, where the Infosphere becomes in itself a human or social ecosystem. It is at that historical moment that it ceases to be simply a network for communication and exchange, but becomes a place of business and human gathering in its own right.

The Infosphere's societal evolution will tend to develop patterns of behavior that grow out of business relationships on the net. Business itself will begin to depart from relational frameworks originally established for *in situ* enterprise environments and will reshape, perhaps even recast, social relationships on the basis of business conducted in a nongeographic, nonphysical, and yet universally accessible environment.

Business will drive the Infosphere's social evolution because it is the serious engine of the new economy being created there. The prevailing patterns of social interaction and relationships will be tied to business development and use of the Infosphere. This is not to say that there are not other, equally important, venues for social and interpersonal development of the Infosphere. These include perhaps the most famous early experiments in social exchange in cyberspace—the online community. And this is not to say that there will not be other drivers eventually of equal or greater force.

The emergence of powerful Internet gateways, or portals, as they are known in the business, suggests that the real affinity in online community may be in shopping. eBay is a tantalizing example of an Internet community built around barter. The sense of belonging, of membership, flows from affinity through economic transaction: people are buying and trading goods from people like them. Consumer

affinity can be enhanced by entertainment affinity (where people have fun with people like them) and news affinity (where people get news from and chat with people like them). The portal companies right now are driving the Internet in this direction just as fast as they can, perhaps rightly sensing a gigantic marketplace. Hence, not so surprisingly, the heady wave in the NASDAQ.

A special piece to the social evolution of the new marketplace is the wild popularity of gaming networks, where groups of players explore worlds of fantasy and fight monsters—or each other!—across this widest area network of all. The millions of young people hooked on online gaming are building social inhabitation in the Infosphere. They are the future inhabitants of this marketplace, and they already live there.[12] Betting on this future explains some of the wild rocketing of Internet stocks.

The millions of young people hooked on online gaming are building social inhabitation in the Infosphere.

It should be of supreme interest that this frenzy of development is fueled by business, that peoples' sense of social affinity even seeks out a business-market place. This is why business enterprise has been such a driver in the American ethos, because business is at the heart of how and why Americans congregate, what they do when they get together, and how they think of themselves. This truth assumes even greater importance because the U.S., after all, is the prime creator and driver of the developing Infosphere. As other cultures engage more extensively in the network world of the Infosphere, other existential cultural factors, like religion, still the driver of many societies, will contend for space and the right to define the new place.

American business, however, will create the social norms and behavioral templates for the first Infosphere era. This is how they might play out:

- Enterprise work relationships, management, and business effectiveness will all be closely watched as a potential foundation for how society as a whole might change its ways to work successfully in the Infosphere.
- New relational patterns will be vested with society-wide authority by their success in the world of enterprise. This means that social norms that work in business will tend to become norms widely accepted and validated throughout society.
- What defines success will be thinking and behaviors that use the new, Infosphere economy to fullest advantage to find jobs faster, to do jobs more effectively, and then move on, building the enterprise all the way.

And this means, in anthropological/sociological terms, building a replacement for the industrial-era ethos through the demonstrable effectiveness of social relationships in enterprise. This leading edge effect in cultural adaptation is not new. It was, in fact, integral to how American society adapted to the industrial big change. What happened then—and what should happen now—is that micro-behaviors, values, and norms established and ratified in business enterprise will aggregate and become in time the explicit basis for the value system of the larger society.

Here is a suggestion as to what three of the new watchwords that sum up Infosphere social norms, values, and behaviors might be:

- **team**—flexibility, openness, less hierarchy
- **task**—organizational fluidity, responsiveness, cross-enterprise
- **trust**—work relationships based on shared value code[13]

What sociologists would call an emerging Infosphere ethos will develop its sense of cultural identity in a new place, adding to its own sense of authenticity and "specialness." The Infosphere's ability to successfully foster a new business culture is critically dependent on the establishment of a sense of shared participation

and belonging in a new setting, environment, or place.

We must underscore again the intrinsically American nature of initial Infosphere cultural evolution. The Infosphere is absolutely global and, eventually, American cultural dominance may recede. We cannot know whether U.S.-established cultural norms will be enshrined as global cultural norms or simply come to represent one of several contending Infosphere ideologies. This outcome, of course, suggests that the Infosphere, as a human place, brings with it all the baggage of all human places, especially the clash of cultures—Us vs. Them—that has been at the heart of all human conflict through history.

The Infosphere's ability to evoke a sense of place is dependent on major, net-global bandwidth expansion. But once it is established, the Infosphere's sense of place becomes an enabler of social migration: the new environment supports a new venue of human activity and, inevitably, a new ethos.

The Infosphere's ability to evoke a sense of place is dependent on major, net-global bandwidth expansion.

Stages of Infosphere Evolution. Phase 2: Governance Shapes the Infosphere

New human places do not organize simply; a new environment and new situational factors are mixed with governing elements carried forward from the old place. There is no such thing as a clean sheet in human culture. As the Infosphere matures and becomes more important in our lives, it will become more and more important to traditional governing authorities also. Traditional governing institutions will seek to extend themselves into the Infosphere, and a new world system, somehow, will root there. The wide-open and informal world of early cyberspace will be replaced by a new web of human arrangements we call civilization: the civic structures of the new place. But in a human ecology without geography, what kind of civic and governing arrangements will we make for ourselves? We describe three notional paths that effort to organize might take. They are not meant to illustrate actual future histories but, rather, to show possible contending dynamics in the evolution of a future world system.

First Notional Path: International fragmentation and ideological division slow Infosphere development

This variant, which could be called a *Maxed-Out World Wide Web*, describes what happens to an Infosphere beset by severe, and interconnected, problems. We identify three problems:

- Restraint by government on free and open transaction in the Infosphere's general, public space through taxation, speech restrictions, encryption controls, and, possibly, capital flow management as well
- Flattening public demand for Infosphere services in reaction to "below threshold" confidence in secure transaction, insufficient privacy safeguards, and telecommunications' enterprise and FCC mishandling of broadband expansion
- International disagreement over issues of access, legal remedy, tariffs, privacy, security, content, and technical standards for the global Infosphere[14]

This emerging Infosphere raises a new world system but it is fragmented and divided, the Infosphere itself a set of separate places, including inaccessible or controlled national intranets. Infosphere space realigns essentially into two camps: the smaller, led by the U.S., is more open, believing in free people and free

trade in cyberspace; the larger, including many old allies, still believes in terrestrial regulation of what people say and do there.

A Maxed-Out World Wide Web is instantly recognizable from today's vantage. But it is not the near-term future. It describes an environment where many of today's most breathtaking possibilities have been cut off or closed down.[15] It attempts to show, by highlighting the major problems that the Infosphere faces, what could happen if all of those problems hit with full force over the next few years.

For these problems to hit with such force, several things would need to happen soon:

- A major rift between the U.S. and the European Union, perhaps surrounding Y2K, or the conversion to the Euro, or a major break with the U.S. over basic taxation and encryption regimes.
- An about-face by the U.S. Government on taxes and regulation of the Internet. This could mean, for example, that FBI moves to counter potential terrorism and organized crime via the network lead to a perception of pervasive surveillance of American citizens, effectively chilling Net gathering. Or this could mean a decision to create an Internet tax regime that would be equally effective in chilling Net commerce.
- A mishandling of how bandwidth and services are delivered to the consumer, where regulatory barriers stifle competition and price broadband out of the reach of most Americans.

This is the most constrained Infosphere future that we discuss; in fact, one could argue whether it is really a global Infosphere at all. In many ways, it has remained only an Internet: it allows people to do research, talk to each other, and have fun, much like today, but the system has stopped short of becoming a global marketplace. Nor does it offer anything like "universal access."

Second Notional Path: A highly regulated, U.S./G-7 managed Infosphere

This variant, which we call the Global Information Infrastructure (GII),[16] describes what might be created by the very steady hand of a world consortium: an international organization emerging from the GII. This environment both benefits from, and is limited by, government regulation. The regulatory regime itself is something of a triumph for traditional nation states and the old, Cold War ideal of an enlightened international system. The GII Infosphere could be described as a G-7 consortium. It is led by the U.S., but its regulatory spirit is more European and Japanese. It achieves, not surprisingly, the most stable and consistent system development. But stability comes at the expense of creativity and liberty. Initiatives not officially approved are forbidden. The U.S. (unquestioned leader of the world consortium) is also the world's unquestioned, almost Olympian policeman. And its authority beat—now that the global economy and its knowledge gather there— is not just cyberspace, but everywhere. But challenges to U.S. authority and the established system come not from the margins, but from the center, and the challenge is not foreign, but domestic.

The GII is instantly recognizable to any Cold Warrior; indeed, it is the Free World alliance catapulted into the Infosphere. But what is its strength is also its weakness. The Free World alliance against the Soviet Empire and its allies drew its authority from the threat the Soviets posed to our collective survival itself. Western electorates allowed their regimes heightened state control during the time of danger. Continuing exercise of this same kind of regulatory control would make for a smoothly coordinated regime in the Infosphere. However, in the absence of a legitimizing external threat, it could soon lack authority among its own people.

Electorates afraid of the unraveling of the welfare state might accept controls on Infosphere liberty if the comforts of the welfare state were also protected in the Infosphere.[17] In Europe especially, but not just in Europe, state authority to regulate the Infosphere would be sustained by fearful electoral majorities.

But only majorities. Dynamic groups driving Infosphere development are angered by the GII. Many who committed themselves to a new world that would shake off the controls of industrial life begin to find themselves back in an old world that has merely migrated to a digital landscape. These builders of the new are not afraid of the fall of the welfare state; many of them would welcome it. And if many of them fought earnestly in the technology trenches of the Cold War, they see no reason why Cold War authority should continue to be exercised over Americans.

Specifically, they resist the intrusive state surveillance that the regime believes is required to police the net. They resist strongly what they see as a threat to basic liberty in the restraint of speech and congregation and contract. And they are ready to rebel at the prospect of the kind of law enforcement and punishment codified in the GII regulations. We might imagine these Infosphere rebels to be strongest right here in the U.S., where traditions of citizen independence, not to mention Infosphere expertise, are strongest. But such a rebellion could soon spread to Europe and Japan.

The problem with the GII is that for it to work, it must effectively assert a global regulatory regime—what many might find a kind of digital tyranny. Hallowed law enforcement traditions tuned to a physical universe quickly break down in a nonmaterial place where anyone can meet anyone, anytime. Patrolling cyber streets, it becomes clear, can only be effective if it is much more intrusive and if police powers are greatly expanded. But exercise of these powers would alienate the most dynamic and creative people in the new Infosphere.

Majority support of a regulated environment in cyberspace is ultimately less important than the support of those who make it run: the Infosphere's builders and users. To the extent that they actively resist the GII regime, the regime begins to delegitimate itself. Creating what amounts to a Singapore in cyberspace, especially in America, might produce a political backlash that could embed rebel factions within the group of nation states running the GII (the G-7). This possibility suggests that this Infosphere, even though it appears orderly and secure on the surface, would intrinsically be at war with itself. Thus, real safety and security would be under persistent low-level attack, with the added irony that terrorism in this situation would equate to political rebellion by its own citizens.

Third Notional Path: An uncontrolled, self-organizing Infosphere ecology

This variant, which we call Byte City,[18] represents a truly liberated, or at least uncontrolled, cyberspace ecology, most likely if enterprise and entrepreneurs continue to dominate the Infosphere as they do today. In one sense, it plays out the arguments of those who started it all; it is revolution through extreme libertarian altruism. All of their theories of how this new world will leave the industrial world's structures of control in the dust, creating a better place, can be put to the test. In another sense, this variant offers a chance to explore what a complex, unregulated human system might come to look like. So the phrase, "complex systems" is meant here to be suggestive, following current schools of thought, of how an initially chaotic human system might come eventually to self-organize, to order itself. But it is also assumed here that the creative force in this elusive process keeps coming out of the U.S. This implies the most challenging [cyber-]terrain for American—national, or tribal?—military

operations. As the creator not only of the Infosphere but also of its highly open regime, the U.S. must attempt to keep its own desired, but fragile, openness workable in an environment that seems to run on its chaos and conflict.

Byte City (they would proclaim in virtuous contrast) shows us how humanity, guided and encouraged by a truly transparent marketplace, can liberate itself. The "oppressive" social structures of the industrial world, as the "digirati" would put it, so necessary to an economy of mass production, will not be overthrown; they will simply no longer be needed. Ideas about Byte City's social evolution unwittingly, and metaphorically, mimic recent scientific thinking about human evolution (especially the school called sociobiology). The existential assumption of the digirati is that the transparent environment of Byte City, like some open market of the soul, will squeeze out all deceit and deception in human relations. Able to see everything, able to hide nothing, means that people will behave truthfully and responsibly at all times—or suffer the (completely public) consequences. So true self-control replaces artificial control from above. Apparent chaos, real order; more civility, actual democracy.

Ideas about Byte City's social evolution unwittingly, and metaphorically, mimic recent scientific thinking about human evolution.

But this is Byte City as its loudly professed "founders" would have it. Byte City would also represent the most complex human ecosystem, combining as it would all human societies in real time and virtual space. If this global social ecology evolves in the absence of traditional social controls, it might well resemble a complex system whose former order has unraveled. The idealized Byte City suggests a noble experiment in living; the real Byte City might look more like old myths from the American West—like Tombstone or "Boom Town."

Perspective

The Byte City environment thus offers a chance to explore what a complex, unregulated human system might come to look like in cyberspace. Problems in the Maxed-Out World Wide Web result from old authorities creating obstacles in the Infosphere's development. Problems in the GII tend to emerge from state regimes' attempts to regulate human activity in the Infosphere. Problems in Byte City come out of its inherent character—its chaos. Just as the control interventions in the GII are ultimately unworkable, so the chaos of Byte City is unsustainable. It is worth exploring the Byte City variant also for what it might tell us about how an initially chaotic human system might come eventually to self-organize and order itself.

These are not, however, like the H. G. Wells novel, intended as "The Shape of Things to Come." These three environments are not meant to suggest serious or complete glimpses of our future. What they try to capture are dynamic human energy surges that will inevitably vie to shape the character of an emerging Infosphere.

So don't think of these stories, global and "future" as they are, as "outcomes." They do not represent sequential environments, nor do they represent a spectrum of best, worst, and most likely. Each "out there" does show how key evolutionary factors can push and pull the Infosphere in very different directions. We need to understand just how different those directions could be.

The breathless building of the Infosphere is driven now by business. This is a phase that could last a decade and more. The formalization of the Infosphere, and the creation of a governable system, is the work of the next phase, which is predominantly civic and political in nature. The three alternative new world systems suggested

here also serve the purpose of reminding us that the next world system—in the Infosphere—will not necessarily hew to traditional models or even the cherished open paradigms of the digital revolutionaries.

We do know that a system is likely to emerge, and the mature Infosphere will have rules and governing contours like our terrestrial world system. In other words, it will be at some level a structured and formalized environment in which equally structured and formalized military activity can, and will, take place. But our thinking about future military activity remains rooted very much in what exists today, like our thinking about the Internet. That is why people talk about "the future of the Internet" rather than the emergence of something very different, like the Infosphere. People like to think of what exists as growing and changing, but it is difficult to imagine really new developments. So in this sense military people think about the impact of the Internet—and all networks—on war and military operations in much the same way that people think about the impact of the Internet on their way of life. Military thought now talks about "network centric warfare," as though this is the future of war. But as we have suggested with popular views about the Internet, it is only a step along the way.

The mature Infosphere will have rules and governing contours like our terrestrial world system.

Our assumption at root is that the impact of the Infosphere on military operations and Defense institutions is ultimately only a subset of the Infosphere's larger impact on society. This relationship holds true as well for almost all technology considerations, where the dominant Infosphere flow is from civilian to military.

INFOSPHERE VS. NETWORK CENTRIC WARFARE

The most advanced thinking in the U.S. Defense world recognizes the process of network migration, where people come to connect primarily in a network environment. They believe, therefore, that future war and military operations will be conducted in the network "ecology." The question is, "Is there a difference between these ideas, which are being discussed widely, and the ideas that we are presenting about the Infosphere, and how are they different?"

The Defense world imagines that someday it will be able to bring data and people together, to see the entire battlefield and control all operations from a shared network. This network is called the Grid. The Advanced Battlefield Information System (ABIS) represents an advanced official view of the future Defense Grid. Here is its definition:

- An "Information Environment," comprising a dynamic, adaptive set of mechanisms, services, facilities, and value-added functions that enable information and knowledge to be developed and exchanged among users and systems in support of their missions.
- Composed of federated systems and elements that can be configured and managed to suit the commander's needs.
- Can be projected globally to support multiple operational areas.[19]

What is needed in this definition is the core truth itself: that the Defense Grid is itself an intranet-extranet that lives as a part of the global Internet. One of the leading thinkers in the Defense world today about these matters, Vice Admiral Arthur Cebrowski, understands this. He also understands that corporate enterprise is pioneering the use of an intranet-extranet paradigm to migrate their business to the

Infosphere. He wants the Defense world to build its own interlocking set of intranets to apprehend and control the world of war the way that, say, WalMart controls the world of retailing or Deutsche Morgan Grenfell the world of securities trading. He talks explicitly about how there is a "shift from viewing actors as independent to viewing them as part of a continuously adapting ecosystem,"[20] showing his understanding of migration ("shift") and human, social place ("ecosystem"). Using his vantage, we might amplify the ABIS definition, suitably updating it:

- An interwoven ecology of "information environments" that are adaptive and supportive enough to create a working social context for people operating in them so that people can do business in these environments much as they do in traditional, physical environments.
- Systems and elements in this ecology can be configured to bring together and support any group of people and any knowledge enterprise.
- This environmental ecology is global and interconnected.

But something is still missing. At its best, the Defense Grid, a network ecology of military intranet-extranets (the extranet part to connect with allies), remains simply military. Much of the thinking about this in the Defense world holds as an unexamined article of faith that it is by definition aloof and pristine. It is a closed system, the "Intersystem,"[21] created for Defense and the conduct of military operations, and thus separate from other networks. Only a few have begun to appreciate the impact of the larger network ecology on the Defense Grid.

Therefore, for much of the thought about network centric warfare, all military-operational activity is constrained to be contained within the Grid. However, the emerging Infosphere is following a pattern of evolution that will absorb the Defense Grid into its larger ecology. The Grid may still operate on its own terms, but it will not be able to operate without reference to the larger Infosphere environment. In fact, the actual situation this future Defense Grid may inhabit (living within an encompassing global network ecology) may make the Grid as currently conceived impossible. In other words, the path to the future described by "Network Centric Warfare" is absolutely correct; it simply hasn't yet gone far enough down the road.

We must add an important codicil to the third element of our definition:

- This environmental ecology is global and interconnected; *no element within the Infosphere—not even military elements—can be truly separated from it.*

This point was made earlier about the impossibility of isolating the DII from the NII and GII. Here are some reasons why it has general and broad applicability:

- **Client-Server Networks → Intranet → Extranet** goes beyond the emerging idea of the Intersystem (the military's Infosphere), and how it is used evolves with the larger society. Business and societies' migration to the Infosphere creates a world in which the military's Infosphere is but a small piece, a compartment somewhat protected from, but completely fused to, the larger whole.
- Civilian social changes will be mirrored across the spectrum of military life and institutions and subcultures. A new business ethos means new, and broadly cast, social relationships, a new *zeitgeist* that permeates and infuses the ethos of military societies too.
- Integration of a developed Defense intranet-extranet (a mature "Intersystem") into global Infosphere society also changes the day-to-day military environment; people are everywhere in the Infosphere, and military personnel live among this larger throng and are intimately connected individually to their larger place.[22]

THE INFOSPHERE'S IMPACT ON MILITARY OPERATIONS?

Operating in an Open Battlespace

Remember, the Infosphere is a seemingly infinite digital ecosystem full of people, and it is an open system. Sure, people's homes and businesses are properly locked and the windows may have iron grills, but the streets are full of people. The Infosphere is like a city, not because it looks like an earthly city but because people live and work there in the same ways they have lived and worked in all earthly cities since Jericho. And military forces are right there too. No longer are soldiers stockaded in isolated posts; no longer are sailors truly at sea. The Defense world may inhabit its own wildly complex web of military intranets, but they will all be tissue-stitched, inevitably, to the larger digital ecosystem.

This means **there will be no one-way extranet**. What do we mean by this? Some have called for an "open Intersystem" while still defining "open" narrowly. There is a tendency to assume that the entire Intersystem would remain pristine, a military intranet of such size and structure that it would resemble the larger Internet but at the same time be at arms' length from it.[23] But the intranet → extranet evolution is equivalent to the creation of a true marketplace/bourse in cyberspace—an infinite public space. If the Defense world is to reach out and seek true, global situational awareness, it must establish itself in this place. As soon as it does this, it loses control of the terms of its interaction with people there.

And this also means **there will be no assured control**—as in situational awareness—no *coup d'oeil.* "Although we believe that our absolute mastery and dominance of today's battlefield will naturally evolve into comparable information-situation control, the Intersystem offers tools for a *coup d'oeil*, the ability of commanders to see and grasp a complex tableau of interacting forces."[24]

There are, however, three basic problems with this expectation. First, there is too much to see: the complexity of the information mass itself will make it impossible to encompass the whole of the Infosphere, just as it is impossible to encompass the whole of human activity on earth. The difference between activity in the Infosphere and on earth is important for understanding Infosphere military operations, because earthly military operations are geographically bounded and limited. Military operations in the Infosphere, a place without geography, must take into account the entire digital ecosystem.

Military operations in the Infosphere, a place without geography, must take into account the entire digital ecosystem.

Second, others will eventually reach our level of info-effectiveness, recreating the offense-defense relationship that has characterized all human conflict environments.

Finally, human presence in the Infosphere is the ultimate complexity. People create an overlay of motivations, behaviors, and knowledge that is too complex to assess.

A corollary issue to operating in an totally open ecosystem will be an increasing *reliance on commercial systems to support U.S. military,* which may create real vulnerabilities. More and more software for American companies is developed abroad. What mischievous code could be embedded there? The consequences of booby-trapped software to U.S. military operations could be quite serious. Likewise, U.S. military communications services could be vulnerable to commercial preemption; that is to say, network services owned by foreign or multinational enterprises could decide, at a moment of crisis, to be unresponsive to military needs. Denial of military Infosphere connectivity could be compared to denial of air space by allies but is actually far more central to the core conduct of military operations everywhere. The

centrality of the Infosphere to military life may require creation of a dedicated, if highly expensive, all-military network architecture.[25]

The problem of the Infosphere is a double-edged sword, benefiting not simply the U.S. but its adversaries as well. A mature, developed Infosphere environment offers subnational entities world-class C4I.[26] This single development would at one stroke change U.S. operational planning and its execution. Suddenly, military operations would be planned and would unfold as if in a fishbowl. All could observe, in real time or near-real time, elements of military planning and, perhaps, much of its execution, creating obvious opportunities for political and military counterattacks to be mounted.

Operating in an Open Human Place

The open architecture of the digital ecosystem also extends potentially to human social behavior there. People living and working in an environment that prizes transparency and access will be everywhere in the way of military activity. Military operations in the infinite bourse or casbah of the global cyber city will resemble military operations in Stalingrad in 1942, or Algiers 1958, or Hue in 1968. People will be everywhere. We could call this the coming problem of *Infosphere operations as MOCUT* (Military Operations in Cyber-Urbanized Terrain).[27] This is because, in the digital ecosystem, military operations eventually, inevitably, get enmeshed in attacking and defending people—what they do, where they live, how they work—and the very structures of life itself.

And this raises another problem. Call it the "Wide-Open Town" problem. The global cyber city will bring all cultures and all governing authorities together in the same place, just as surely as it will bring together all people, knowledge, and business. Imagine the potential for constant conflict, all without boundary between anyone's old sense of "foreign" and "domestic." American military forces will likely be in a state of near-continuous operations throughout this environment, and not simply in discrete, targeted, protected little "frontline" niches like Bosnia or Haiti or Somalia. The blur of war and peace now extends beyond "unconventional," "peacekeeping," "anti-terrorism"; it extends to *a constant tempo of ongoing Infosphere operations*. For analogies, think of a police department in a great, metropolitan city too chaotic to control—like Rio or Cairo; think of colonial administration in, say, the Congo Free State in 1900, with a few officers to cover a million square miles; or active, ongoing frontier operations, well below the threshold of war, but demanding and deadly —say, the Northwest Frontier of British India. Or just remember the Westerns you used to watch on TV as a kid and how so many took place in that "wide-open town," not yet really civilized, not yet a fit place to raise a family. That just might sum up the Infosphere in its coming, early days.

The Symbiosis of Physical and Cyber Operations

So far, it might make sense. But perhaps the hardest leap of faith required for thinking about military operations in an Infosphere-centered world is this: fighting simultaneously in both digital and material worlds. In fact, it is harder even than that: human activity in the digital ecosystem will be symbiotically intertwined with physical activity on earth. There are no "flash of recognition" analogies to help us think through how this digital-physical weave will actually work; it goes way beyond the telephone or E-mail, way beyond sharing data across a WAN or LAN. The overriding truth of the symbiosis means that breaking it becomes perhaps one of future war's most cherished goals. And the mesh of digital and physical also means that war, and the intense tempo of operations that we associate with 20th century combat, migrates along with us to the Infosphere.

- Evolution of a doctrine of **"an initial period of Infosphere operations."** War becomes a high-stakes' gambit for Infosphere control, with high-intensity Infosphere operations as a concept that might achieve the initial goal.
- Development of an **"Infosphere defense suppression campaign."** The strategic problem of an initial period of Infosphere operations has its tactical corollary: How to disable enemy defenses? Defense suppression in the Infosphere is not straightforward; it is not as smooth as a bolt from Olympus, or from today's info-warriors—stunning and singeing all before it in a world where the U.S. rules cyberspace.
- **An evolving target-set.** First stage, today, we think of the Infosphere as advancing our ability to hit physical targets; second stage, the physical nodes of the Infosphere; third stage, C4ISR of others in the Infosphere; fourth stage, the softer elements that support C4ISR, the civilian information network; fifth stage, the public square that is the Infosphere itself.

Military Societies Transformed

Does the evolution of a new business ethos in the context of a new economy or, in shorthand, a *team-task-trust* business paradigm, change military organization? Without trying to detail outcomes, some obvious changes might be suggested, such as a general leveling of authority and a necessary streamlining of command hierarchies. It will simply not be possible to maintain multiple layers of management and organization when they are absolutely unnecessary and, in fact, destroy battle efficiency. The Infosphere thus becomes a destroyer of intermediate levels of command. Familiar, even comfortable, command hierarchies will be brought down, for not only will they no longer be needed, they will actually and materially impede the conduct of operations. Command to front line will be direct, instantaneous, and secure: no intermediation required. The challenge then will be: What to do with all those mid-level jobs?

If the Infosphere encourages a new military environment in which war-peace operations are blurred even more than they are today and in which MOCUT operations are an inherent part of the total operations' environment, then severe consequences for personnel can be suggested too, such as

- Different recruitment sources
- Different military-professional profile
- Different military lifestyle and social organization

These could lead to a conundrum that military societies, and the entire Defense world, must eventually face:

- If the military tries to stay big, then it will become increasingly vulnerable to the very world it must operate within.
- Does a military becoming small need to create an ethos separate from the rest of society if it is to keep military effectiveness?

AND THE IMPACT ON THE NAVY?

There is no doubt that moving toward the Infosphere will mean great leaps forward for the Navy. Vice Admiral Cebrowski's idea of network centric warfare shows persuasively how naval capabilities will benefit. But beyond benefit, pure and simple, are other potential impacts on the Navy, and these need to be looked at.

Relating to the Navy's Unique Identity

Navy identity was existentially shaped by an independence of naval units from shore control. This enforced autonomy defined a naval service that was distinct not only from the body of a military organization ashore but also from the entire social-administrative structure of national command.[28] The telegraph began a long erosion of this tradition. By the end of the 20th century, navies seem no different from any other military units in the field. They are naval now

only in the sense that they operate ships at sea. As the conduct of all military operations migrates to the Infosphere, some may say that ships themselves have become even more subsidiary to central military action. They will admit that ships remain essential as mobile weapons' platforms, but a new Defense world dominated by Infosphere operators may think of these platforms as shooters only, a la the late-arsenal ship. And it will be hard to argue with the new "info-warrior" class, for the Infosphere will have an ever-increasing capacity to achieve a local battle picture without relying primarily upon a ship's onboard sensors and to make tactical decisions without depending primarily upon a ship's own input. Call this the flip side to the bonus network centric warfare brings the Navy, but it must also be confronted.

Relating to the Viability of the Ship Itself

The Navy will undoubtedly come under political attack because navies and their ships always seem to come under political attack in times of great technological change. But this time, unlike earlier anti-Navy campaigns that focused on the "obsolescence" or "vulnerability" of the Capital Ship, this political fusillade will take aim at the ship itself. This in turn may foster a broader, if softer, perception that the ship (and thus the Navy!) is a less valued element in the national arsenal.

This will be a perception that must be strongly countered because it will seem on the surface to make sense; because, in fact, the world of the Infosphere will be a world exposed. Sensor nets will proliferate: almost all physical terrain (as well as cyber-terrain) will be visible and able to be tracked down, by almost anyone. What we regard as "world-class C4ISR" today will be accessible by individuals, not just states, and certainly, not just great powers.

Today's classic combatants, tracing their lineage back to the beginning of this century, may have to change dramatically to stay viable in a physical world dominated by a cyber-world. Certainly they will need the most robust defenses. And they must be convincingly robust, not just to adversaries but to naysayers in the Defense world, the media, and Congress (but it must be remembered that this is not a new or especially insurmountable problem; navies have been dealing with it since the advent of iron and steam).[29] The ships, or at least some of them, may also have to become smaller, stealthier, or more deceitful: able to disguise themselves as supertankers or commercial carriers.

What we regard as "world-class C4ISR" today will be accessible by individuals, not just states, and certainly, not just great powers.

Relating to the Navy's Own Emphasis on Strike Warfare

By stressing strike warfare and operations in littoral areas, the Navy may be adding fuel to arguments that the Infosphere will diminish the Navy identity. Strike warfare and littoral operations seemed a perfect way to enhance Navy centrality in a post–Cold War world of Major Theater Wars (MTWs). However, since Desert Storm, the compelling possibility of another imminent MTW has declined. Strike warfare becomes limited strike operations, and littoral warfare becomes peacekeeping operations. The Infosphere's rise lends historical force to a canonical shift in the business of future war, as the Infosphere intrudes itself more and more into human conflict and as the activity of human conflict itself migrates to the Infosphere.

Look just at one dimension of the shift: targets. The "target" came to define industrial war, but look now at how target "sets" change! Infosphere targets may become the highest value targets in a world of highly select target sets. Naval delivery of ordnance on these targets may still, in this context, be the preferred delivery,

but how does the Navy begin to redefine itself the best delivery platform, especially if that platform differs fundamentally from traditional Navy strike platforms?

What the Infosphere's emerging proponents may argue is the metamorphosis of a navy of independently capable ships to a navy of highly capable, but essentially weapons, platforms. We said earlier that the Navy has been existentially defined by the ship. If the Navy is to survive being "defined down"[30] by the Infosphere, it must adapt to the Infosphere in an existential way. This means that for the Navy to effectively respond to the Infosphere, it must do more than simply add on, plug in, or upgrade Infosphere features. Much more. The question of the Navy and the Infosphere is an existential question of renewing the society of the ship, and of a sea service. And although this may be a profound question, it is not necessarily an unbearably difficult question.

The answer lies in (1) demonstrating why local, on-scene integration of "battlespace awareness" remains important, and (2) showing how distributing Infosphere battle assets (through "Infosphere combatants"!) enhances overall strategic robustness.

The question of the Navy and the Infosphere is an existential question of renewing the society of the ship, and of a sea service.

Integrated Battlespace Awareness

We can imagine an Infosphere-driven world where there will be sensors everywhere, and where galaxies of tiny sensor nets can be cast over any theater.[31] Tomorrow's info-warriors will certainly go even further than this, insisting that the Infosphere can integrate all local sensors and effectively feed their data to local weapons systems. However, bringing sensors to the environment, and connecting sensors surely to the shooter, will always be a special problem, especially when the shooting starts. A warship has no problem bringing sensors to the battlespace, nor has it a problem connecting sensor to shooter. Warships are packages. But there's more than that involved. The Infosphere-driven world will bring new challenges to situation awareness. Will we always be able to determine when information operations are being conducted against us? New tools to assess the information environment will be needed, as will new ways of conveying situation awareness to commanders.

Strategic Robustness

Talking about ship vulnerability is easy and familiar; we have been doing it for centuries. But talking about Infosphere vulnerabilities will be very hard, at least until the first big Infosphere-centric war sorts things out. Our confidence in the robustness of U.S. military assets in the Infosphere will be wholly untested. Yes, the Infosphere will be an intensely dense and redundant network ecology, but the Defense Infosphere's ability to sustain a real-time battlespace picture and necessary target data feeds will be unknown. We should not forget that critical Infosphere assets may reside in fixed, ground-based sites, at half a world's remove from American "shooters." The ship, in contrast, remains a mobile sensor-shooter package, able to defend itself and synthesize its own battle picture on scene. The ship retains the necessary on-board skills to both back up and validate locally the encompassing mosaic picture offered by the Infosphere and its global galaxy of off-board sensors. This will remain important because the larger Infosphere fire control environment may be vulnerable, both to sensor and network degradation, and to sensor and network deception.

But the ship offers more than tomorrow's battle backup. The ship, like warfare clay at its most plastic, can be molded anyway we want,

not just in terms of HM&E, of course, but in combat system terms as well. The Navy can, if it wishes, mold tomorrow's Infosphere combatant: a warship that exists authoritatively in both terrestrial and cyber-battlespace. If the Infosphere environment is without geography, then anyone, anywhere can enter the Infosphere without regard to geography. This may suggest that military operations can conveniently be centralized, or it may suggest just the opposite. Why must operations be orchestrated, and command exercised, from top-heavy shore establishments? Why not now do these things from a node as efficient as a ship? The ship is, as always, the vessel of a Navy society reinventing itself, adapting as it has time and time again to change on land, so it can still stay at sea.

If the Infosphere environment is without geography, then anyone, anywhere can enter the Infosphere without regard to geography.

AND ON PROFESSIONAL INSTITUTIONS?

Research and development institutions in the national security arena, such as JHU/APL, will play a key role in assisting military societies' migration to the Infosphere. But the roles they play in encouraging Defense adaptation to a new world will be shaped first by the larger, and fundamental, shifts that the Infosphere will bring to military operations and Defense concepts in their broadest sense.

We have suggested that the maturing Infosphere could change our traditional notions of military operations and national Defense concepts dramatically. Specifically, these canonical changes might include:

- The end of a pristine military-information environment. American Defense information "warriors" live today in a mental universe of total, assured control. System threats are at once marginal, like the hacker threat, and exist only at our sufferance. If we choose to pay attention, and "throw some resources at the problem," it will go away. What we are saying is that, in the world of the Infosphere, it will not go away.
- The end of assured U.S. battlespace control. If anything, the sense of absolute control is even great among strategic operators, who cannot even begin to imagine that our future information grids might be limited, damaged, or even brought down by enemy action. But that is exactly the historical prospect that the mature Infosphere holds out to us, and a long-term strategic challenge that the U.S. must face. That is exactly why "dumb ships" (platforms than function only in traditional "weapon space") are dangerous and why integrated and distributed Infosphere-sensors-weapons platforms—real warships, to us—will be needed in a competitive Infosphere future.
- Military operations in the Infosphere will be shaped by, and unfold within, the global city (MOCUT). Not only will U.S. military operations be challenged in the Infosphere, they will take place in a jostling, crowded, noisy, and compromised social environment that may be surprising, and even dismaying, in its intimacy. U.S. forces will operate and fight cheek-to-jowl with the world, not the CNN broadcast world of Gulf War cliche but a far more intrusive audience of millions. Much military effort will go to masking the movement of U.S. forces, safeguarding their deliberations and throwing the scent off their ultimate intent.

This is what we mean by fundamental changes, the kind of changes that force military societies to adapt existentially, because the very reality they exist in has changed and because, to be effective in this new human reality, the basis of military identity must change too. Existential adaptation means that military societies must think of themselves first and foremost as

societies and not simply as organizational entities:

- They should see the interplay of technology and society as the larger process of cultural change.
- They should see social migration and reconfiguration, also, as a larger, adaptive cultural process. They, too, will need to adapt, potentially changing basic building blocks within their societies, from organization, to people's roles and relationships, to management.
- They should see that basic changes are possible in intra- and international relationships, including fundamental changes in both the American and world systems.

The technology potential and challenges of the Infosphere in no way obscures the issue of the fundamental change it brings to institutions, and how our own organizations, as little societies, will eventually deal with the big change that is sweeping over all society. In the Defense world (itself only a subset of our larger world), core change in military societies becomes a cultural cascade, spilling down to affect the life and roles of technical organizations with equal power, showing how the Infosphere brings corollary changes to technical societies.

Enterprises are already using the Internet to speed products to market by exploiting time zone differences that allow virtual round-the-clock development. For example, one company has software written in India, which can be reviewed in the U.S. while the Indian developers are sleeping at home. Work days can be stretched without resort to multiple shifts, still speeding product development. Other companies are using collaborative design and engineering on the Net to improve product quality, putting their best people on a project, and it doesn't matter where in the world they live.

This kind of big change in the commercial world means change in other worlds too. So the Infosphere will transform people's roles and relationships in Defense organizations. We have treated some of these changes and would like to suggest one additional issue here: the potential impact of the Infosphere on collaborative analysis, design, development, assessment, and operational support. Capabilities of the Infosphere will free teams from physical and organizational "place," allowing teams to work together free from these heretofore immutable limitations. While this allows the active involvement of world-class expertise in pursuing tasks, use of the best available tools (such as computer simulations), and access to the most complete and up-to-date data (regardless of where these resources may reside), it also creates entirely new social and management issues. Addressing them will be essential not just to effectiveness and efficiency but also to survival in the new world of the Infosphere. But given the staid character of many in the Government R&D community, and the inertia they can muster to fight change, many may find this transition difficult.

Capabilities of the Infosphere will free teams from physical and organizational "place."

CONCLUDING COMMENTS

The Infosphere promises to transform war, not by replacing battle as we know it but by folding military operations into a new condition. We use the word, "condition," because the yet unveiled new war is more than a new environment; it is a new experience, demanding totally new mindsets and behaviors. That this condition is not visible makes responding to its possibility difficult. That this condition will emerge from the larger society and its culture only adds to the difficulty. We face a revolution in war that may equal or surpass the big change in war brought by the Industrial Revolution, but

everything about this change makes it hard for military societies to respond.

We can also say that when such a change comes, decisive response to it is essential. Adaptation is survival. So the big question for today's Defense world should be: How do we prepare ourselves for the change? How do we learn to adapt, so that when the change comes, we can change too?

We face a revolution in war that may equal or surpass the big change in war brought by the Industrial Revolution.

Fortunately, the big change hasn't happened quite yet, so there is still time, though perhaps not a lot of time, to get ready. And fundamentally, adaptation is all about mental attitude. So in the time remaining before the transformation, military societies should concentrate their change efforts on changing their own attitudes about change, rather than trying to make changes. Thinking, not action, is what is needed now.

Why just thinking? Because open thinking is probably the hardest thing for the Defense world to do right now, before the change, because open thinking means being open to its consequences. Everyone knows big change doesn't simply end the status quo; it can end whole rice bowls, whole programs, whole agencies, whole military services. Remember horse cavalry?

So how do we tackle thinking itself? We suggest a mental exercise. Thinking about the composition of our military forces is something we all do. Perhaps we can approach the implications of big change by contrasting possible future military forces. For example, if big change was distant, a remote possibility in time of social and technology stagnation, how would we approach building our forces for the future? This is the easy part: threat analysis, external environment assessment, all reasonably straightline-able, thanks to a stable technology context.

Now think about a future military force for an entirely different world. Take our whole bundle of hypotheses and wrap them up in the Infosphere. What kinds of forces and capabilities might the U.S., or the whole U.S.-centric world, for that matter, need in a world that does its business primarily in the digital ecosystem? The straightline will not take you there, thank you; to the contrary, you must break the line entirely and start somewhere else on the chart. Or better still, make a new kind of chart.

What kinds of forces and capabilities might the U.S., or the whole U.S.-centric world, for that matter, need in a world that does its business primarily in the digital ecosystem?

Finally, the future military force path helps us think. We know we face big change, so we can't straightline. We don't know where the change will take us, or when, or how, so we can't actually plan an "Infosphere military force." But we can describe a third path: that of a military force for the time right before the change, the "cusp military force," if you will. It is here that crucial thinking must happen, because shaping a military force for the time right before a big change means building in adaptability. Thinking through actual force planning in a time of extreme change is, ultimately, not just an exercise in thinking about how to adapt.

It is adaptation. It is the first step along the path to change. It is not necessarily the change we would like, but it is the necessary change that lets the Navy continue. And by "continue" we mean this: that the Navy gets to keep what it values most—its identity, its very self—even as all the physical things around it swirl out of recognition. But the Navy ensures its future only if it confronts the Infosphere now. Because the crisis of the Infosphere is but a few short years away.[32]

Appendix A
Infosphere Aspects — How and When?

Our discussion of the Infosphere and military operations needs a suggestion of how and when the Infosphere might actually emerge. What follows is our best sense of the next 10 years, watching the Infosphere evolve, tracking its development by using the six relevant benchmarks shown below, the thresholds that must be crossed for the Infosphere to really arrive. For each, we speculate on when (starting from mid-1999), the factors involved, the outcome of crossing the threshold, and the military Impacts.

1. Economic barriers to Infosphere entry
2. Majority participation in the Infosphere
3. Bandwidth watersheds
4. Processing watersheds
5. Business application watersheds
6. Dominant social acceptance/use threshold

1. Economic barriers to Infosphere entry

When: 2 years; based on industry ramp-up to competition

Factors: An awaited period begins in which the computer and telecommunication industries are fused and recast. This distinct historical process kick-starts a multi-dimensional, passionately competitive information market—blurred, chaotic, and with impacts much bigger than any possible in former markets. This is a high-intensity period of industry restructuring, characterized by massive investments and many mergers.

Outcome: All this activity and investment means equally high levels of bandwidth expansion. Like 19th century railroad boom periods, frenetic competition means very rapid growth of the network. The peak energy period may be historically brief, but can result in high growth multiples in network and in throughput.

Military Impacts: Government spectrum offers the potential for an enormous expansion of military bandwidth. One path to expansion is through arrangements that piggyback off of civilian investment, trading and swapping for pieces of the new architecture. Also, fearing being left behind, explosive growth in civilian investment could spur competing Government investment.

2. Majority participation in the Infosphere

When: 3 years

Factors: (1) Personal computer penetration of consumer market: low-end PCs (200+ MHz Pentium) now crashed the $1000 consumer "sweet spot" over 6 months ago, and PCs in the sub-$600 and sub-$300 categories are driving penetration now. This period may be even briefer than suggested here. PC penetration into the home was forecast in 1998 as 53% by 2000; that level was reached in January 1999. The threshold for creating Infosphere connection as a social norm ideally is about 70%, a market level possible a year or so thereafter.[33] (2) ISP connection/fast modem costs should be roughly equal to cable TV and TV purchase, i.e., ~$30/month and $300–$500. In January 1999, AOL announced a planned DSL service for $30/month. Entering the Infosphere should be about as demanding and stressful socially as, say, using a VCR was in the mid-1980s. Then, people joked, but people used.

Outcome: Hitting these thresholds creates, in effect, a social realignment in society where Internet use is no longer for college kids and

elite parents but something everyone does as a normal part of everyday life. The ~30% of those not using will have made the decision to stay behind or will be buying and using very soon. Infosphere use as a norm means that it translates into a social pressure that only adds to its momentum.

Military Impacts: Once the public passes the social threshold of majority use, the military will accelerate toward more emphasis on the larger, public network. This will be because (1) this will be where the information is, and the high-value economic activity, and the "bad guys," and (2) this will be where most service personnel are hanging out, both in their job and off duty.

3. Bandwidth watersheds

When: 3–5 years

Factors: An aggressively competing mix of xDSL (@~1.5 mbps), cable modems (@3–10 mbps), and wireless (@~1.0 mbps). The era of 56K and ISDN will be essentially gone.[34] Network access will be closing in on universal, a faster ramp-up—because of competition—than introduction of cable TV.[35] Forecasts peg xDSL subscribers at just under 3 million by 2003, with 6.2 million cable modem households. Ten million subscribers would be only a fraction of online households, the narrowness of the slice being driven in large part by people's currently expressed aversion to pay more for broadband. Current data show that only 10% of today's online households would be "very likely" to pay $40/month for high-speed access, while 25% say they would be "somewhat likely." That 10% ties in nicely with current projections on broadband market penetration. It must be stressed, however, that AOL's announced lowering of the bar (to $30/month), and historically decreasing bandwidth costs, could change the collective mind very quickly. Add to this the potential appeal of a high-speed connection once some people in every neighborhood have it. And it must be said, finally, that for digital subscriber lines, the old telecommunications giants have been very less than agile.[36]

Outcome: Supports full-motion, high-quality video (30 frames/second); permits smooth delivery and seamless integration of real-time virtual environment update packets to the user.

Military Impacts: Civilian expansion piggybacking plus USG backbone investments could mean mega-mip bandwidth for all military activities—a capacity that in itself will encourage evolution of the Grid into military Infosphere turf.

4. Processing watersheds

When: 5 years

Factors: (1) Multi-processing/1000 MHz as the CPU low end (based on long-established trend lines, now apparently continuing, unabated, with copper in the chip). (2) Modern, stable, multi-threaded, multi-tasking operating systems; Linux, OSX, NT 5 replace OS crop with roots in the computing world of the late-1970s.[37] Then, a second iteration of these will be needed, this time emphasizing ubiquity of communication and interoperability in the Infosphere: everything talks to everything! (3) Desktop metaphor goes away, with its keyboard-centric, office origins; replaced by metaphor of place, through which user moves as walking, or in flight. (4) This transition actively encouraged by appearance of mature, ubiquitous 3D visualization tools, integrated within the OS and its application suites. The Internet becomes a place, with the PC box or HDTV as its gateway; the Internet thus shape shifts into an Infosphere, where the PC-space defines a personal reception area, ante-chamber, or lobby for the user, connecting the user's private space (office, lounge, etc.) with the outside (Infosphere) world. (5) Software engines that represent users as virtual humans, rather than crude avatars, will be widely available. Full-frame, streaming video will be the standard.

Outcome: People will be able to enter and move easily within the newly created place. Users will also be able to meet others easily in the Infosphere or receive them in their personal spaces. The use of virtual human representation, although available, may not gain immediate popularity. It will be far easier for people to accept the Infosphere as a place than it will be for them to accept digital emissaries, *avatars*, as socially adequate substitutes for their masters, *real people*. It is more likely that high-quality, big-window video will remain the norm for several years.

Military Impacts: The "placeness" of the Infosphere will affect military society in several ways. (1) The Infosphere will cease to be a medium for select and specialized "info-warriors"; everyone can go there. (2) The way it is used by military groups, and the scope of operations conducted there, will grow as more and more of the public world's activities migrate there. (3) Because the network is available to all, it is possible to offer equivalent information sets at all command levels. Traditional hierarchies and ways of doing business will encourage leadership to control information and access, but, in fact, the opposite will occur. Operational effectiveness will require hierarchy downsizing, especially in military middle management. It will also require more info-sharing across command levels.

5. Business application watersheds

When: 7 years

Factors: Infosphere growth is being driven by business utility. The rapid growth of enterprise intranets is a result of the immediate productivity gains they offer. But as high bandwidth becomes the norm in business, before it is available to the consumer, its ability to achieve instant, long-distance, distributed social connection will encourage enterprises to do more and more of their internal business in the intranet Infosphere. The corporate intranet is also rapidly becoming a productive avenue for connecting to customers—through enterprise extranets. The 7-year benchmark is based on 70% of corporate business occurring on the intranet and 50% of external business on corporate extranets.[38]

Outcome: (1) Business use established the Internet-Infosphere as a compelling and attractive place. It also creates certain market momentum, as millions who work daily in high-bandwidth offices begin to want the same when they get home. (2) Business use of the Infosphere also creates a compelling model for non-business applications and legitimates an aggressive migration to Infosphere by groups and institutions that otherwise might have been very reluctant emigres. (3) Business use is also social use. Business exchange and interaction in intranet and extranet is creating the parameters for productive social connection there.

Military Impacts: Civilian models for productive social exchange and interaction in the Infosphere will be adopted by military society. Military education will model itself on civilian university patterns in the Infosphere; research methods will follow those pioneered for general use in the Infosphere; military work patterns will tend to follow the most successful models in civilian enterprise. All of these changes in aggregate will mean potentially fundamental changes in military society itself.

6. Dominant social acceptance/use threshold

When: 10 years

Factors: When primary/secondary education becomes routine in the Infosphere (following its development in the university); when the typical office environment is now defined as an Infosphere office (local physical offices will increasingly occupy a declining social status, almost as part of a bygone era); when most commerce and shopping occur in the Infosphere

(including groceries and other rapid-delivery, low item value consumer markets); when all research-oriented communication and data inquiry happens in the Infosphere.

Outcome: The social-cultural flow can be likened to a great, historical migration. Traditional places do not go away but, rather, are integrated into a new environmental tapestry in which the Infosphere represents the premier place, the place of high value and high status.

Military Impacts: (1) Military society migrates also to the Infosphere, where most command, management, military education, and military intelligence now take place. Concentrated military office complexes are no longer needed, and personnel and logistics management is altered radically. Fewer physical bases are needed. (2) "Bad guys," along with everyone else, now can aspire to potentially world-class C4ISR, as it was understood in the late-1990s. U.S. C4ISR must now recreate itself at a much higher level of security. Security becomes the main effort. Active military operations to ensure effective and secure U.S. C4ISR will be ongoing, at potentially demanding levels. (3) U.S. military personnel are, like the rest of American society, integrated personally and professionally into the global Infosphere. They are now at risk of casual and directed attack, wherever they are, all the time. Defensive and offensive operations in defense of our military people will absorb an increasing share of investment and energy.

Appendix B
JHU/APL and the Infosphere — Selected Items

Leaders at The Johns Hopkins University Applied Physics Laboratory (JHU/APL) began to wrestle with Infosphere implications in early 1997. They could see first-hand how Cooperative Engagement Capability (CEC), which JHU/APL helped pioneer, is changing naval operations.[39] Some from JHU/APL had also taken part in the Advanced Battlefield Information Systems (ABIS) Task Force,[40] which raised proto-Infosphere questions. Their growing awareness led them to support an Infosphere Seminar Project early in 1997 to think most broadly about what the future might bring. This project's very design was to expand on issues already addressed by network centric warfare analyses and publications to bring out the full range of possible Infosphere implications for the Defense world.

The Infosphere Seminar Project began with a seminar for JHU/APL leadership in April 1997 that had three objectives: (1) identification of Infosphere technology implications; (2) identification of Infosphere technology opportunities; and (3) implications of Infosphere Operations and Infosphere Warfare. Two general scenarios offered an operational context for discussion: (1) a precision strike mission in a peace-keeping mission, and (2) power projection operations in a major regional conflict. Three Infosphere variants were considered. These were designated as (1) Maxed-out World Wide Web (WWW+), (2) Global Information Infrastructure (GII), and (3) Byte City. They defined a range of possibilities in which the impact on military operations and organizational structures could be explored. The April seminar was followed by a seminar for JHU/APL cyber-specialists in May.

These seminars developed many insights, both about military operations and about JHU/APL's own functioning. They underscored the importance of working in an Infosphere environment. An Infosphere-engaged workforce, and deft leadership, will increasingly determine JHU/APL's value to the Defense community. Any effective research and development organization will have to have Infosphere compatibility in its policies, organizational and environment.

JHU/APL has shared its insights from the Infosphere Seminar Project seminars with others in the Defense world, beginning with Infosphere sessions at the Naval War College (November 1997) and at the Joint National Test Facility (December 1997), and carrying on with this report. JHU/APL continued its exploration of Infosphere implications by the Cyber Tech Seminars that started in the spring of 1998. In these seminars, leaders from various information enterprises shared their visions of the future in public forums and discussed their implications in seminars with their peers. Materials generated by the sessions can be accessed via the Cyber Tech Seminar button at the bottom of the JHU/APL external home page (URL: **http://www.jhuapl.edu/**) or accessed directly at the Cyber Tech Seminar Web site (URL: **http://www.jhuapl.edu/cybertech/**). The topics and speakers of the first series of Cyber Tech Seminars are shown below.

CT-1 (April 8, 1998) Cyber Threats and Information System Security Seminar

Special Agent James V. Christy, IV (IPTF/AFOSI), *How to Protect Your Infrastructure from Information Attacks*

Mr. Keith Rhodes (GAO), *Computer Security Issues & Year 2000 Issues*

CT-2 (June 30, 1998) Building the Cyber Place: Internet Bandwidth & Architecture Issues

Dr. Stephen Wolff (Cisco Systems), *Taking a Guess at Tomorrow's Internet*

Mr. Tim Regan (Corning, Inc.), *Fiber Optics*

Mr. Greg Gum (U S WEST, MegaBIT Services), *The Future of Broadband Technologies: An xDSL Perspective*

Mr. Douglas Dillon (Hughes Network Services), *The Future of Satellite Communications in the Digital World*

Mr. John Montjoy (GTE Internetworking), *Summary Comments*

CT-3 (August 6, 1998) A New Window on the World

Dr. James Gosling (VP/Fellow, Sun Microsystems Chief Scientist, Java Software), *JAVA, Building a Connected World*

Dr. James Waldo (Jini Architect, Sun Microsystems), *Decentralized Control in a Federated Network*

Mr. Alex Cone (President, Director of Sales, CodeFab), *CodeFab*

Mr. George A. Spix (Chief Architect, Consumer Platforms Division, Microsoft Corp), *Concluding Remarks*

CT-4 (September 25, 1998) Connecting the World

Mr. Mark Kusiak (Technical Director, Advanced Programs, Lucent Technologies), *Perspectives on Networking Bandwidth*

Mr. John Bowles (President & CEO, ADVOCAST) & Mr. Eric Keith (Vice President, Sales, ADVOCAST), *ADVOCAST, The Advocacy Network*

Mr. Carl M. Ellison (Senior Security Architect, Intel Corporation), *Raising the Security Bar*

Mr. Charlie Robertello (Vice President, Mid-Atlantic Region, SecureIT, Inc. [VeriSign Inc.]), *Network Security Solutions*

CT-5 (November 13, 1998) The New Cyber Landscape

Dr. David S. Ebert (Professor, Computer Science & Electrical Engineering Department, University of Maryland, Baltimore County), *Perceptually Motivated Information Visualization*

Mr. Sherman Woo (Director, U S WEST's Global Village Media Center), *Imagineering Cyberspace*

Dr. Andrew Hunt (Staff Engineer, Speech Applications Group, Sun Microsystems Laboratories), *JAVA Speech API*

Dr. W. Bruce Croft (Professor, Department of Computer Science, University of Massachusetts, Amherst), *Information Retrieval in the 21st Century*

Dr. Stephen G. Eick (CTO, Visual Insights, Lucent Technologies), *Information Visualization*

CT-6 (February 9, 1999) Making It Happen: High Performance Computing

Dr. Thomas Sterling (Senior Scientist, NASA Jet Propulsion Laboratory), *From Toys to Teraflops: The Emergence of Commodity Supercomputing*

Dr. George Paul, Jr. (IBM Thomas J. Watson Research Center), *Deep Blue: Chess Rematch*

Dr. Jayadev Misra (Professor, Dept. of Computer Sciences, University of Texas at Austin), *Computing on the Internet: Concurrency, Distributed Objects and Safety Guarantees*

Dr. John D. McCalpin (Principal Scientist, System Architecture Group Silicon Graphics Inc.).

Dr. Paul Messina (Senior Advisor, Department of Energy Accelerated Strategic Computing Initiative [ASCI]), *Ushering in the Era of Terascale Scientific Simulations*

NOTES

[1] In a prepared statement before the Senate Governmental Affairs Committee, Washington, D.C., June 24, 1998, Lt. Gen. Kenneth A. Minihan, Director of the National Security Agency (NSA), emphasized that the U.S. must regard the threat of cyber attack with the same degree of intensity as it viewed the potential nuclear threat during the Cold War <**http://www.defenselink.mil/pubs/di98/di1343.html**>. A similar perspective is reflected in the phrase, "Weapons of mass disruption will rival weapons of mass destruction"—a sort of hortatory banner at the Information Operations Technology Center (IOTC), an organization sponsored by both the Defense Department and the Intelligence Community. This phrase might be likened to an early battle cry of the digital warrior. Similar sentiments are reflected in the May 1998 Presidential Decision Directive (PDD) 63 on protection of the nation's critical infrastructure.

[2] Throughout this report we use "network" as a shorthand for the entire spectrum of advances in information technology (computer hardware, software, and all kinds of associated devices, e.g., displays, cameras, speakers) as well as advances in communications, switches, and network architecture that could make the capabilities sketched here, reality.

[3] Thinking of a human network, integrating people and their activities, as an ecosystem, is a metaphor first bequeathed to capitalism by Michael Rothschild in *Bionomics*, New York, Henry Holt, 1990. The ecosystem metaphor has been picked up by leading military thinkers in this domain. See Vice Admiral Arthur K. Cebrowski and John J. Garstka, "Network Centric Warfare: Its Origin and Future," *Naval Institute Proceedings*, pp. 28–35, January 1998. This modern variation on the classical comparison with Nature can be appealingly pasted onto the Infosphere, like an Amazon in the ether—a complete world, from silicon fiber substrate to digital canopy.

[4] Military societies are beginning to take this view also. See Rear Admiral Robert M. Nutwell, "IT-21 Intranet Provides Big 'Reachbacks,'" *Naval Institute Proceedings*, pp. 36–38, January 1998. However, economic advantage has not always driven the evolving Infosphere. Initially technology drove its roots for a couple of decades after initiation of the ARPANET, and it is unclear what may drive a more fully developed Infosphere, as we show later.

[5] The underpinnings of American ethos are treated authoritatively in Rodney Stark, *Sociology*, 6th Edition, Wadsworth, 1995.

[6] Richard A. Barrett, *Culture and Conduct: An Excursion in Anthropology*, Wadsworth, 1984.

[7] Thinking about information operations is already emphasizing this point. At the Third Combat INFOSEC Symposium (March 1998) one speech noted that the Defense Information Infrastructure (DII) can be isolated neither from the National Information Infrastructure (NII) nor from the much larger Global Information Infrastructure (GII). Recent testimony by the DoD Chief Information Officer (Arthur Money) and Deputy Defense Secretary John Hamre to House Armed Services Committee Procurement and R&D Subcommittees emphasized that the DII must be restructured into a defendable Global Networked Information Enterprise, Daniel Verton, "DoD Revamping Massive Information Architecture," *Federal Computer World*, 1 March 1999.

[8] Michael Vlahos, "The War After Byte City," *Washington Quarterly*, pp. 41–72, Spring 1997.

[9] John Langton and R. J. Morris, eds., *An Atlas of Industrializing Britain 1780–1914*, Methuen, 1982.

[10] For testimonials to the brief heyday of the elite "cyber-community," see Howard Rheingold and John Perry Barlow, "Community in Cyberspace?" *Utne Reader*, pp. 51–64, March–April, 1995; for a look at the much more demotic and commercial-centric online gathering places of today, see Robert Hof, Seanna Browder, and Peter Elstrom, "Internet Communities," *Business Week*, pp. 63–85, 5 May 1997.

[11] From NUA Internet Surveys: "Email users are expected to double between now and the year 2000, surpassing the 108 million mark. These users are expected to receive more than 7 trillion messages per year." <**http://www.nua.ie/surveys/**>.

[12] Marc Saltzman, "Super Games!" *the net*, pp. 21–40, August 1997; Richard C. Waters and John V. Barrus, "The Rise of Shared Virtual Environments," *IEEE Spectrum*, p. 25, March 1997; or, for a flavor of life among the Quake Clans, see <**http://192.41.38.217/thepress/index.htm#Player Profiles**> or <**http://jord.sbc.edu/dragon/frames.htm**>.

[13] That these concepts would come to define us in the Infosphere is an argument made most forcefully in a lyrical passage from Peter Huber's, *Orwell's Revenge: The 1984 Palimpsest*, The Free Press, pp. 171–181, 1994.

[14] The European Union Privacy Directive, for example, could effectively create a powerful nontariff trade barrier for e-commerce between the U.S. and the European Union. See Peter P. Swire and Robert E. Litan, "None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive," Brookings, 1997. <**http://www.acs.ohio-state.edu/units/law/swire1/noyb.htm**>.

[15] History is replete with technical and social examples of backward movement, from the loss of Aristarchus' heliocentric view that Copernicus rediscovered nearly two millennia later to China's rejection of European industrial technology in the 19th century.

[16] Details about the GII may be obtained from the GII website <**http://www.gii.org:80/index.html**>. It is a "politically correct" expectation of the future, with its familiar National Information Infrastructure (NII) and Defense Information Infrastructure (DII) elements.

[17] Why would the U.S. give in to European plans to turn the Infosphere into a highly regulated environment? Because the U.S., especially its still-traditional Cold War establishment in Washington, fears loss of leadership. Major clashes loom between U.S. instincts to keep the Internet a totally open system and determined European Union plans to run the emerging Infosphere as tightly as French cheese. Successive trade/regulatory wars could be seen as eroding American leadership in Europe over time. Today's Washington establishment places supreme store in preserving American military and political chieftainship. It might accept European Union Internet regulations in return for law enforcement/national security control of the Infosphere. Encouraging this is a trend within the Cold War establishment for assessing new threats in the Infosphere itself. Terrorism and international crime are seen as tomorrow's threat growth areas.

[18] Relative to the Byte City concept, see <**http://www.usic.org/infosphere**>.

[19] ABIS Task Force Report, 1-1. The 1996 Advanced Battlefield Information Systems (ABIS) Task Force **<http://www.cs.tamu.edu/zhao/abis/abis.htm>** was a study sponsored by the Director of Defense Research and Engineering (DDRE) and the Director, Command, Control, Communications, and Computer Systems (J6) of the Joint Chiefs of Staff. The charter of the ABIS Task Force was to stake out the technology demanded by Joint Vision 2010.

[20] Vice Admiral Arthur K. Cebrowski and John J. Garstka, "Network Centric Warfare: Its Origin and Future," *US Naval Institute Proceedings*, pp. 28–35, January 1998.

[21] Martin Libicki, "The Intersystem: or, The RMA Reified," National Defense University Institute for National Security Studies, Draft Version 0.5, May 1997.

[22] There are antique harbingers of this. During Desert Storm, in the floppy era, at least one military computer was infected by a computer virus that decreased its military utility because military personnel inserted an infected disk into the computer to play a computer game.

[23] This assumption is nicely presented in John Garstka, "The Emerging J-6 Strategy for Information Superiority," J63-S&T, "beta version."

[24] Libicki, *op cit*., p. 33.

[25] It will probably be impossible to fully support all military functions with a dedicated, all-military network, especially if logistics are included, given the dependence of military logistics upon civilian systems. Those nonmilitary aspects of the network would become vulnerabilities that an astute adversary might exploit. It makes little difference whether supplies fail to reach military commanders because the adversary has bombed a bridge or because adversary information operations have gridlocked the transportation system.

[26] Space does not allow a full description here of future C4I for small nations, subnational entities, non-government organizations, or individuals. However, the Infosphere's clear potential to eventually offer these capabilities widely means that this possibility should be given serious consideration.

[27] This is a play on acronyms, but also a reminder of how quickly basic doctrinal emphases can change. MOUT (Military Operations in Urbanized Terrain) emerged out of the Vietnam War's wreckage of American military thought and the search for a meaningful doctrine of war. This culminated in the later 1970s in the creation of Field Manual 100-5. MOUT was an integral component of a new conceptual focus on war.

[28] Carl H. Builder, "The Masks of War: American Military Styles in Strategy and Analysis," A RAND Corporation Research Study, The Johns Hopkins University Press, 1989. Builder makes the point well: "Tradition has always been an important part of military life, but the Navy, much more than any of the other services, has cherished and clung to tradition. . . . the Navy looks to its traditions to keep it safe. If tradition is the altar at which the Navy worships, then one of the icons on that altar is the concept of independent command at sea, which, like the Holy Grail, is to be sought and honored by every true naval officer. . . . Independent command of ships at sea is a unique, godlike responsibility unlike that afforded to commanding officers in the other services. Until the advent of telecommunications, a ship 'over the horizon' was a world unto itself, with its captain absolutely responsible for every soul and consequence that fell under his command." (p. 19).

[29] Michael Vlahos, "A Crack in the Shield: The Capital Ship Concept Under Attack: 1885–1975," *The Journal Of Strategic Studies*, 1979.

[30] As used famously by Senator Daniel Patrick Moynihan in his philippic,"Defining Deviancy Down," *Miles to Go: A Personal History of Social Policy*, 1997.

[31] Martin Libicki painted this picture several years ago.

[32] Two appendixes complete this report. The first explains when and how we believe various aspects of the Infosphere will manifest themselves. The second

provides information about JHU/APL and the Infosphere.

[33] "Lower Priced PCs Hit the 'Sweet Spot,'" *Wall Street Journal*, 12 September 1997. Two-thirds of U.S. households will have internet access by 2003, according to research by the Yankee Group (<**www.yankeegroup.com/yg.nsf**>: "Consumer Demand for Internet Access Booming," 23 March 1999).

[34] U.S. West has already offered xDSL connections in 40 cities in the Western U.S. Cable modem bandwidth is shared, so that typical throughput averages in the 1.5–3 mips range.

[35] From discussions among industry leaders at a summer conference held in Aspen, Colorado, Cyberspace and the American Dream IV, 15–17 August 1997.

[36] Louis Trager, "Broadband Disappoints Customers," *Interactive Week*, p. 8, 7 December 1998; Carol Wilson and Louis Trager, "High Speed Data Deliverance: Is It Do or Die In '99 for ADSL?," *Interactive Week*, p. 53, 1 March 1999.

[37] "The Media OS," Technical White Paper, <**http://www.be.com/products/beos/mediaos.html**>.

[38] From NUA Internet Surveys: "An International Data Corporation market research survey of 175 large companies reports 46% are planning to employ E-commerce on their Internet web sites [22 May 1997]. ZDNet reports that Forrester Research predicts business-to-business commerce will grow three times faster than business-to-consumer commerce. CommerceNet predicts business-to-business transactions will represent 25% of all Internet commerce by 2000. A 1997 FIND/SVP survey indicates 60% of all business users get onto the Web every day [20 May 1997]." <**http://www.nua.ie/surveys**>.

[39] "The Cooperative Engagement Capability," *Johns Hopkins APL Technical Digest*, **16**(4), 377–396, 1995.

[40] As noted earlier, the 1996 Advanced Battlefield Information Systems (ABIS) Task Force <**http://www.cs.tamu.edu/zhao/abis/abis.htm**> was a study sponsored by the Director of Defense Research and Engineering (DDRE) and the Director, Command, Control, Communications, and Computer Systems (J6) of the Joint Chiefs of Staff. The function of the ABIS Task Force was to explore technology expected for and required by Joint Vision 2010.